Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-14 (Canceled).

Claim 15 (New): A method of detecting virus infection of an executable image, the method comprising:

determining the file type and the entry point of the executable image;

scanning the executable image, with reference to a database of start-up code characteristics including patterns characteristic of start-up code generated by known compilers used to create respective file types, for start-up code at a location other than said entry point generated by one of the compilers used to generate the determined file type; and

flagging the executable image as suspicious from the point of view of possibly containing a virus infection in response to it being determined during the scanning that the executable image contains said start-up code at a location other than said entry point.

Claim 16 (New): A method according to claim 15, wherein the database of start-up code characteristics includes records of data values associated with routines which form part of the start up code, and

the step of scanning the executable image for start-up code comprises identifying the data in the executable image corresponding to at least one such data value and comparing it with that value.

Claim 17 (New): A method according to claim 15, further comprising:

performing remedial action in respect of executable images flagged as suspicious from the point of view of possibly containing a virus infection.

Claim 18 (New): A method of detecting virus infection of an executable image, the method comprising:

determining the file type and the entry point of the executable image;

determining, with reference to a database of start-up code characteristics including patterns characteristic of start-up code generated by known compilers used to create respective file types, whether the executable image has at said entry point code similar to start-up code generated by one of the compilers used to generate the determined file type but with the beginning of this code having been changed; and

flagging the executable image as suspicious from the point of view of possibly containing a virus infection in response to determining that the executable image has said code at said entry point.

Claim 19 (New): A method according to claim 18, wherein

the database of start-up code characteristics includes records of data values associated with routines which form part of the start-up code, and

the step of determining whether the executable image has at said entry point code similar to start-up code generated by one of the compilers used to generate the determined file type but with the beginning of this code having been changed comprises identifying the data in the executable image corresponding to at least one such data value and comparing it with that value.

Claim 20 (New): A method according to claim 18, further comprising:

performing remedial action in respect of executable images flagged as suspicious from the point of view of possibly containing a virus infection.

Claim 21 (New): A system for detecting virus infection of an executable image, the system comprising:

a file-type analyzer operative to determine the file type and the entry point of the executable image; and

a start-up code searcher operative to scan the executable image, with reference to a database of start-up code characteristics including patterns characteristic of start-up code generated by known compilers used to create respective file types, for start-up code at a location other than said entry point generated by one of the compilers used to generate the determined file type,

the system being operative to flag the executable image as suspicious from the point of view of possibly containing a virus infection in response to it being determined by the start-up code searcher that the executable image contains said start-up code at a location other than said entry point.

Claim 22 (New): A system according to claim 21, wherein

the database of start-up code characteristics includes records of data values associated with routines which form part of the start-up code, and

the start-up code searcher is operative to identify the data in the executable image corresponding to at least one such data value and comparing it with that value.

Claim 23 (New): A system according to claim 21, wherein the system is operative to perform remedial action in respect of executable images flagged as suspicious from the point of view of possibly containing a virus infection.

Claim 24 (New): A system for detecting virus infection of an executable image, the system comprising:

a file-type analyzer operative to determine the file type and the entry point of the executable image; and an entry point code analyzer operative to determine, with reference to a database of start-up code characteristics including patterns characteristic of start-up code generated by known compilers used to create respective file types, whether the executable image has at said entry point code similar to start-up code generated by one of the compilers used to generate the determined file type but with the beginning of this code having been changed,

the system being operative to flag the executable image as suspicious from the point of view of possibly containing a virus infection in response to determining that the executable image has said code at said entry point.

Claim 25 (New): A system according to claim 24, wherein

the database of start-up code characteristics includes records of data values associated with routines which form part of the start-up code, and

the entry point code analyzer is operative to determine whether the executable image has at said entry point code similar to start-up code generated by one of the compilers used to generate the determined file type but with the beginning of this code having been changed is arranged to identify the data in the executable image corresponding to at least one such data value and comparing it with that value.

Claim 26 (New): A system according to claim 24, wherein the system is operative to perform remedial action in respect of executable images flagged as suspicious from the point of view of possibly containing a virus infection.